(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

C3

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75782 A1

(51) International Patent Classification[7]: G06F 11/22, 11/273, 1/00

(21) International Application Number: PCT/GB00/02082

(22) International Filing Date: 31 May 2000 (31.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9912817.5 2 June 1999 (02.06.1999) GB

(71) Applicant and
(72) Inventor: CARTER, Nicholas, Peter [GB/GB]; 19 Spicewood, Fareham, Hants PO15 5EX (GB).

(74) Agents: BERESFORD, Keith, Denis, Lewis et al.; Beresford & Co., 2-5 Warwick Court, High Holborn, London WC1R 5DJ (GB).

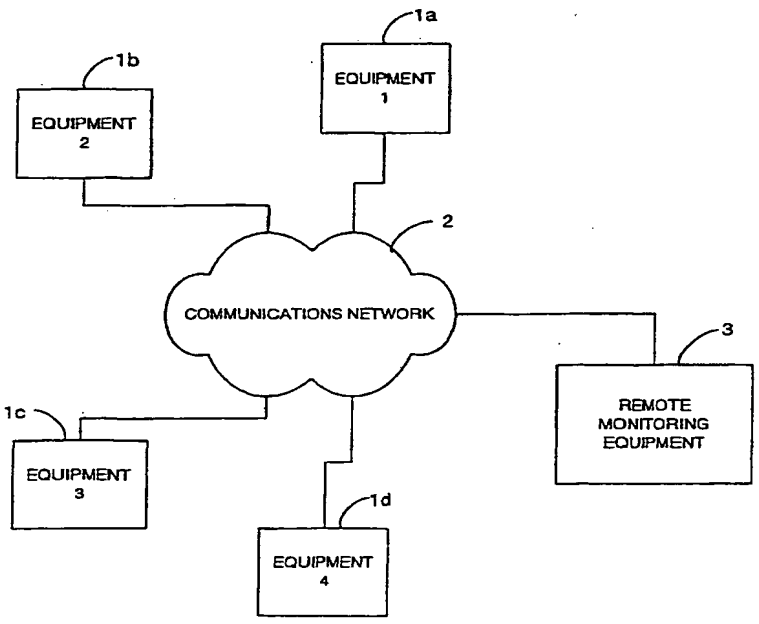
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURITY SYSTEM



(57) Abstract: A security system keeps a record of configuration information for apparatus at a monitoring station. Changes in the configuration information for the apparatus is monitored by the apparatus and the changes are transmitted to the monitoring station. This enables the monitoring station to quickly assess whether the configuration changes are indicative of a security breach and if so to take appropriate action.

WO 00/75782 A1

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F11/22 G06F11/273 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 287 505 A (CALVERT NATHANIEL ET AL) 15 February 1994 (1994-02-15) abstract; claims 1-6	1-40

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 October 2000	10/10/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sarasua, L.

Form PCT/ISA/210 (second sheet) (July 1992)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75782 A1

(51) International Patent Classification[7]: G06F 11/22, 11/273, 1/00

(21) International Application Number: PCT/GB00/02082

(22) International Filing Date: 31 May 2000 (31.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9912817.5 2 June 1999 (02.06.1999) GB

(71) Applicant and
(72) Inventor: CARTER, Nicholas, Peter [GB/GB]; 19 Spicewood, Fareham, Hants PO15 5EX (GB).

(74) Agents: BERESFORD, Keith, Denis, Lewis et al.; Beresford & Co., 2-5 Warwick Court, High Holborn, London WC1R 5DJ (GB).

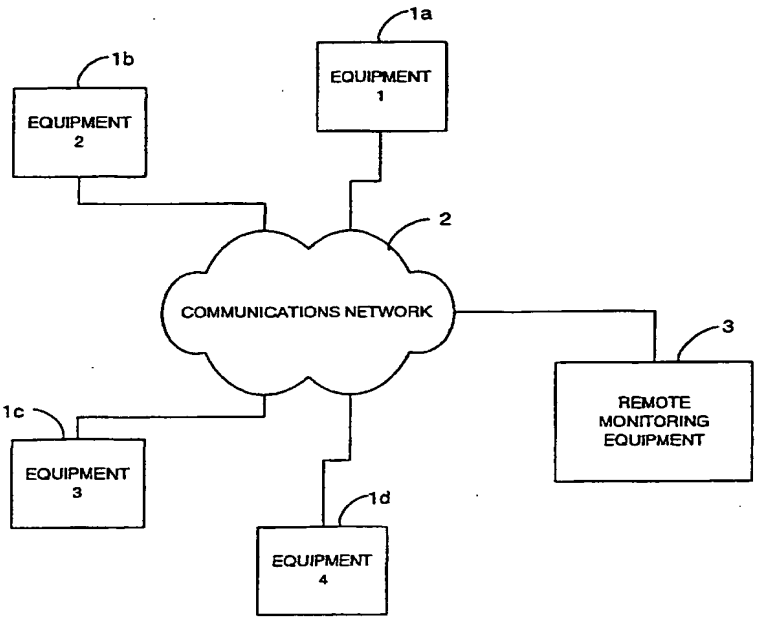
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURITY SYSTEM



(57) Abstract: A security system keeps a record of configuration information for apparatus at a monitoring station. Changes in the configuration information for the apparatus is monitored by the apparatus and the changes are transmitted to the monitoring station. This enables the monitoring station to quickly assess whether the configuration changes are indicative of a security breach and if so to take appropriate action.

WO 00/75782 A1

SECURITY SYSTEM

The present invention generally relates to a security system for monitoring the change of configuration of equipment indicating the possibility of a security breach. The present invention also relates to an equipment auditing system.

With the increasing prevalence of high value, high technology equipment, it has become a problem for managers to keep track of equipment. The maintenance of an audit for equipment for example owned by a company can be extremely laborious. This is particularly the case with regard to computers where it is desirable to maintain an audit of both hardware and software owned by a company. In view of the ever present problem of software piracy, it is particularly important that the company should keep an accurate software audit.

Another problem with high value, high technology equipment is the problem of theft. For example, theft of computer equipment has become a problem. Various techniques have been used to try to reduce this problem including electronically tagging computers, and providing security markings.

The problem with the security marking technique is that it only becomes useful when the computer equipment is recovered since it aids identification of the owner.

The problem with security tagging is that it adds costs since it requires complex tagging equipment.

It is an object of the present invention to overcome the problems with the prior art.

A first aspect of the present invention provides a method of monitoring apparatus by keeping a record of the configuration information for the apparatus remote from the apparatus. Configuration information for a number of apparatuses can be stored. Within the apparatus the configuration of the apparatus is monitored in order to determine any changes. When changes occur in the configuration of the apparatus these are transmitted to remote monitoring equipment.

The configuration information for the apparatus can provide a "signature" unique for the hardware and the use to which the apparatus is put. Further, where the apparatus is programmable, the configuration information can give a "signature" for the software configuration of the apparatus. The configuration information can include details on the user and details on the location of the apparatus.

For security purposes, the technique can be applied by only transmitting changes within the configuration information which are pertinent to security. The designation of certain information parameters as pertinent to security will be dependent upon the apparatus and the use to which it is put.

In an embodiment of the present invention the configuration information for the apparatus is automatically determined and transmitted to the remote monitoring equipment at some initial stage. In this way the remote monitoring equipment can store a database of configuration parameters for a number of apparatuses.

Thus with the transmission of changes in configuration information for apparatus, when this changes, the remote monitoring equipment is able to keep an up to date database of configuration information for a number of apparatuses. This therefore provides an efficient automated auditing system.

In addition to the auditing system, an embodiment of the present invention provides a security aspect by requiring the user to register by submitting manually entered configuration information for the apparatus. This can be compared with the automatically transmitted configuration information in order to identify a discrepancy. This feature of the present invention provides insurance companies for example, with a means for confirming that the insured party has correctly specified the insured equipment and thus avoids insurance fraud.

The configuration information for the apparatus can include a large number of parameters and is dependent upon the apparatus. For example, the configuration information can include information on the hardware components of the apparatus, and information on the use of the apparatus by a user. This latter information can provide information on a pattern of use of the apparatus by the user. When monitoring for security breaches, a considerable change in the pattern of use of the apparatus by the user can indicate breach of security e.g. theft of a computer, because an unauthorised user

will use the apparatus in quite a different way from an authorised user.

Where the apparatus comprises computer equipment, the configuration information can include information on the software loaded on the computer.

Preferably the present invention is intended to operate covertly. Thus the determination of changes in configuration information and the transmission of the changes are not apparent to a user to avoid the possibility of an unauthorised user overriding the transmission of the changes which warn of a security breach.

Apparatus which includes means of communication is able to directly communicate with the remote monitoring equipment in order to transmit the changes in configuration information. Examples of such apparatus are mobile phones, and other computer equipment equipped with a modem or network card for connection to a local area network.

Where the apparatus does not include means for transmission to the remote monitoring equipment, the apparatus includes means to output the changes in association with information or instructions which are intended for input to another apparatus. Thus, the changes are output together with instructions to cause them to be transmitted as a package attached to information or instructions output from the apparatus. This package thus acts as a virus or trojan in a computer system. When an apparatus receives the package, if it has

transmission means, the package is activated and transmits the changes. If the apparatus does not have a transmission means, the package is simply passed on as an output attached to information. In this way the package is propagated between computers until it is transmitted successfully to the remote monitoring equipment.

In accordance with a further aspect of the present invention there is provided an automatic audit system in which apparatus configuration information is transmitted from a plurality of apparatuses to an auditor station. Changes in the configuration information for the apparatus are monitored by the apparatus and these changes are transmitted to the auditor station. In this way the auditor station keeps an accurate record of the configuration information for the apparatuses.

Embodiments of the present invention will now be described with reference to the accompanying drawings, in which:

Figure 1 is schematic diagram of a generalised embodiment of the present invention;

Figure 2 is a flow diagram illustrating the operation of the embodiment of Figure 1;

Figure 3 is a schematic diagram of a computer in accordance with a first embodiment to the present invention;

Figure 4 is a flow diagram illustrating a first method of installing the program to implement the embodiment of Figure 3;

Figure 5 is a flow diagram of another method of installing the program to implement the embodiment of Figure 3;

Figure 6 is a flow diagram illustrating the operation of the embodiment illustrated in Figure 3;

Figure 7 is a flow diagram illustrating in more detail the transmission step S46 of Figure 6;

Figure 8 is a schematic diagram of a network embodiment of the present invention;

Figure 9 is a flow diagram of the method of installing the software in the network embodiment of Figure 8; and

Figure 10 is a flow diagram of the steps carried out in the implementation of the embodiment of Figure 8.

A generalised embodiment of the present invention will now be described with reference to Figures 1 and 2.

As can be seen in Figure 1 a number of pieces of equipment 1a, 1b, 1c and 1d are connected to a communications network 2 and thereby to remote monitoring equipment 3. The communications network 2 can comprise any means of communication to remote monitoring equipment e.g. a telecommunications network requiring direct dialling by each piece of equipment 1a, 1b, 1c and 1d to the remote monitoring equipment 3, the internet requiring each of the pieces of equipment 1a, 1b, 1c and 1d to have an internet connection, or a wireless network such as a cellular network for mobile telephones.

Each of the pieces of equipment 1a, 1b, 1c and 1d have unique configuration parameters which are dependent upon any one of a number of parameters such as hardware, software and the use to which the equipment is put by the user.

The operation of the embodiment of Figure 1 will now be described with reference to the flow diagram of Figure 2.

In step S1 the user of the equipment 1a, 1b, 1c or 1d registers with the party operating the remote monitoring equipment 3 and submits configuration information which has been entered manually. For example, the user is required to provide details of the hardware and software provided at the equipment together with personal details.

In step S2 the user then loads the security program onto the user's equipment and in step S3 the security program determines the configuration information and the equipment and transmits it to the remote monitoring equipment 3. At the remote monitoring equipment 3, the submitted configuration information is compared with the transmitted configuration information to determine if there are any discrepancies in step S5. If there is a discrepancy, in step S10 the party operating the remote monitoring equipment 3 will contact the user to try to clarify why this discrepancy has arisen. Thus the facility greatly enhances the ability of an insurer to detect insurance fraud. The remote monitoring equipment 3 can be operated by an insurer and an insured party can

be required to install the security program as well as submit information on the equipment that they wish to insure. Any discrepancy between information submitted and information automatically detected may indicate an attempt at insurance fraud.

Thus, the remote monitoring equipment 3 stores configuration information for each of the pieces of equipment 1a, 1b, 1c and 1d thus enabling the auditing of the equipment. This has great benefits where the system illustrated in Figure 1 comprises a company computer network i.e. the communications network 2 comprises a local area network.

Having obtained the initial configuration information from each of the pieces of equipment 1a, 1b, 1c and 1d, the security program then proceeds to monitor the equipment in step S6 and in step S7 it detects whether there are any changes. When changes occur, in step S8 the equipment transmits the changes to the remote monitoring equipment 3. In this way the remote monitoring equipment 3 is kept up to date with all configuration changes and thus maintains an up to date audit.

In a computer system, there are many reasons why the configuration parameters may change. For example, at each of the pieces of equipment 1a, 1b, 1c and 1d, new software may be installed, or a user may change the hardware configuration e.g. by adding new hardware. The nature of these changes can indicate whether there has been a security breach e.g. whether there is unauthorised

use of the equipment such as when the equipment has been stolen. Thus in step S9, the party operating the remote monitoring equipment 3 can consider whether the changes are significant i.e. pertinent to security. For example, the mere fact that new software has been loaded need not be an indication of a security breach. However, change of a user name, change of user personal details, or change of connection parameters may point towards a security breach and could thus lead the party operating the remote monitoring equipment 3 to contact the user in step S10.

If the changes are not considered significant in step S9, the process returns to step S6 whereby the security program continues to monitor the equipment.

A specific embodiment of the present invention will now be described with reference to Figures 3 to 7.

Figure 3 schematically illustrates a computer for use in this embodiment of the present invention. This embodiment can be implemented using a multipurpose general computer suitably programmed. The computer comprises a conventional computer bus 10 linking conventional components of the computer together i.e. pointing device (mouse) 11, the keyboard 12, the display 13, the processor 14, the modem 15, the volatile memory 16, and the disk storage medium 17. The processor implements process steps stored as computer program modules in the disk storage medium 17. The volatile memory 16 is provided as a working memory for use by the processor 14. The modem 15 is provided to enable

transmission of configuration information to a remote monitoring station (not shown).

This embodiment of the present invention illustrates the data structure used by the Microsoft Windows 95™ operating system. The Windows 95 operating system uses a data structure termed the system registry which stores configuration information required by or used by the hardware of the computer and by the software implemented on the computer. The structure of the system registry in the Windows 95 operating system is well documented in text books and will be familiar to a skilled person in the art. However, a brief overview will now be given.

The system registry comprises a data structure presented to a user of the operating system as though it was a file structure. However, the entries in the registry are not stored as a file structure. The only files which are stored permanently in the disk storage medium 17 are the system.dat and the user.dat files. The system.dat file contains configuration information for the hardware and software which is not specific to the users. The user.dat file contains configuration information which is specific to the or each user of the computer. When the computer is booted up, the permanently stored system.dat and user.dat files are copied to temporary files user.da0 and system.da0. These are used as the working copies of the files whilst the computer is running. Using these files the registry data structure is provided to the user as can be seen in

Figure 3. The registry is presented as a data structure having keys. The six keys of the registry are:

HKEY_CLASSES_ROOT

HKEY_CURRENT_USER

HKEY_LOCAL_MACHINE

HKEY_USERS

HKEY_CURRENT_CONFIG

HKEY_DYN_DATA

Each of the keys has a number of subkeys each of which have subkeys etc. In this way the keys are arranged as a data structure.

The HKEY_CLASSES_ROOT key contains object linking and embedding (OLE) information and information about the relationships that exist among file classes.

The HKEY_CURRENT_USER key contains a user profile of the user who is currently logged on. This information includes environment variables set by the current user and the user's personal program groups (desk top settings, network connections, printers, and application preferences).

The HKEY_LOCAL_MACHINE key contains information about the local work station currently in use, including startup control data and hardware and operating system data. The hardware information includes data about the local work stations desktops, the systems memory, and device drivers used by the system. The HKEY_LOCAL_MACHINE key is formed from the data in the user.da0 file on the disk of the disk storage medium 17. The subkey classes under the subkey software of the key HKEY_LOCAL_MACHINE

key is used to form the entries in the HKEY_CLASSES_ROOT key.

The HKEY__USERS key is currently loaded user profiles, including the one maintained in the HKEY CURRENT_USER key. The HKEY_USERS key is formed from data stored in the temporary system file system.da0 stored on the disk storage medium 17. The HKEY_CURRENT_USER key is always a subkey of the HKEY_USERS key and is always a default profile.

The HKEY__CURRENT__CONFIG key is mapped from a specific configuration in the HKEY_LOCAL_MACHINE key.

The HKEY_DYN_DATA key stores dynamic data for the current system configuration and maintains a set of performance statistics that show how the system is running. The data for this key is never stored on the disk storage medium 17 and is only ever kept in the volatile memory 16.

The registry can be treated as a file system and is addressable as if it were a file system. The inventor of the present invention has realised that because of this it is possible not only to store information in the registry but also store program code. As can be seen in Figure 3 in this embodiment a new subkey SECURITY has been added under the HKEY__LOCAL__MACHINE key. The SECURITY subkey has itself two subkeys PROGRAM and DATA. The PROGRAM subkey stores the program code for execution by the processor 14 to implement the embodiment of the present invention. The DATA subkey stores a copy of the HKEY_LOCAL_MACHINE key data and the HKEY_USERS key data.

Thus the program can be addressed using "MYCOMPUTER/ H K E Y _____L O C A L MACHINE/SOFTWARE/CLASSES/SECURITY/PROGRAM".Because the security program is stored as a subkey in the HKEY_LOCAL MACHINE key, it is stored in the system.dat file when the computer is shut down and it can thus be accessed using a disk address.

In the registry it is possible to hide entries. This further reduces the possibility of the security program being detected and thus circumvented by someone trying to breach security.

By installing the security program in the Registry, it is made more difficult for someone trying to circumvent the security procedure. The file is hidden. The registry is a very large and complex data structure and thus only experienced computer users would have a chance of locating the program as a key in the registry. This is of course, assuming that they are expecting to find it. Further, because it is not stored as a file, it cannot easily be deleted. For example, it is not possible simply to delete all files and reinstall Windows 95. The registry files system.dat and user.dat are stored as hidden files on the hard disk and when Windows 95 is reinstalled, it looks for these files stored on the disk so that it can use a previous copy of the registry.

Two methods of installation of the security program will now be described with reference to Figures 4 and 5.

Figure 4 is a flow diagram of a first method of installation of the program. In step S20 the set up

process is initiated for example, by entering a floppy disk with the initialisation program installed and typing the command "setup.exe". In step S21 the security program code is copied to the new subkey PROGRAM under the SOFTWARE subkey of the HKEY_LOCAL_MACHINE key. In step S22 a registry entry for the program to run on bootup is then added and in step S23 the computer is rebooted. During reboot the system.dat file is updated using the temporary system file (system.da0) during the reboot operation in step S24. The computer then runs on bootup in step S25. In the method illustrated in Figure 4 the installation program is able to directly copy the security program code into the new key in the registry.

Figure 5 is a flow diagram illustrating an alternative embodiment in which the set up process does not directly copy the security program code into the registry but instead installs a program which can do so.

In step S30 the set up process is initiated and in step S31 the installation program and security program code are copied to a folder on the disk. In step S32 the installation program is run and in step S33 the security program code is copied to a new subkey PROGRAM under the SOFTWARE subkey of the HKEY_LOCAL_MACHINE key. In step S34 the registry entry for the program to run on bootup is then added and in step S35 all registry entries for the installation program and the security program code in the folder are deleted together with the folder itself. The computer is then rebooted in step S36 and in step S37 the system.dat file is updated using the temporary system

file (system.da0) during the reboot operation. Following the reboot operation the security program is then implemented (step S38).

Thus in this embodiment of the present invention, the security program is installed in the registry so as to run on bootup to identify changes in the configuration information for the computer.

The operation of the security program will now be described with reference to Figures 6 and 7.

When the computer undergoes bootup in step S40, in step S41 the security program determines whether the DATA subkey has a data entry. If not, the data in the LOCAL_MACHINE and USERS keys are transmitted to the remote monitoring equipment in step S49. In step S50 it is then determined whether the transmission has been successful. If not, the program can periodically retry to transmit in step S51. After a predetermined number of unsuccessful retries, the program will terminate in step S53. If in step S50 the transmission had been successful, the LOCAL_MACHINE and USERS data will be copied to the new DATA subkey in step S52 and the process will then terminate in step S53.

Thus, the security program will only store the data in the DATA subkey if it is sure that the remote monitoring party has successfully received the data. If it has not, the program does not store the data and the next time the computer is booted up, steps S49 to S52 will be repeated.

Thus steps S49 to S52 provide a means by which a remote monitoring party can automatically receive configuration information for the computer. This can be used for auditing purposes as well as for security monitoring.

If in step S41 there is a data entry present in the DATA subkey, in step S42 the data in the LOCAL_MACHINE and USERS keys are compared with the data in the security programs DATA subkey in the registry. In step S43 it is then determined if there is a difference. If there has been no change in configuration the security program terminates in step S43. The method by which the comparisons can take place in step S42 is by a simple text string comparison. The data can be identified by the key path, the name of the data (since each key can contain more than one data item) and the data content itself as:

path|name|data|

where the data has been deleted, the text for comparison can be given by:

path|name| |

Thus, by simply comparing each of the data structures given above consecutively, for the data in subkeys of the HKEY_LOCAL_MACHINE and the HKEY_USERS keys, differences can be identified.

If however, there are changes, an optional step S44 can determine whether these changes are "critical". If they are not critical, the program may terminate in step S53.

The reason for the optional step S44 is to provide a means for screening out configuration changes which are not pertinent for security. In an implementation for auditing purposes, all configuration changes can be transmitted. However, for a security implementation, it may be desirable only to transmit changes which are considered to be significant. In order to set the changes which are considered to be "critical" it is simply necessary to flag keys which are pertinent to security. The following list some of the keys for which changes could be critical.

CRITICAL CHANGES

1. Change of machine name or ID

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ ComputerName\ComputerName

2. Change of internet service provider (ISP)

HKEY_USERS\Default\RemoteAccess\Addresses - (This gives the services (remote or ISP names))

HKEY_USERS\default\RemoteAccess\Profile\ISPName\ Terminal - (This gives the phone number)

HKEY_USERS\Default\RemoteAccess\ProfileISPName\User - (This gives the account name).

3. Change of network connection

HKEY_LOCAL_MACHINE\Network\Logon - (This gives the log on name)

4. Change of remote connections

This is the same as for 2 above.

5. Dialling code and phone number changed

HKEY_USERS\Default\Software\Microsoft\WindowsMessaging Subsystem\Profiles\MSExchangeSettings\ d27c21ebe56f.../001e3a09 - (This gives home phone number)

HKEY_USERS\Default\Software\Microsoft\WindowsMessaging Subsystem\Profiles\MSExchangeSettings\ d27c21ebe56f.../001e0c1f - (This gives home fax number)

6. Change of users

HKEY_USERS - (Any user added or especially deleted after default).

SUBTLE CHANGES

1. Settings for MS Mail

HKEY_LOCAL MACHINE\Software\Microsoft\AtWorkFax\LocalModems\General\LocalId - (This gives fax number).

2. Services for MS Mail

All the subkeys under:

HKEY_CURRENT_USERS\Software\Microsoft\WindowsMessaging Subsystem\Profiles\MSExchangeSettings

3. Changes in program use (i.e. new applications loaded or old ones deleted)

All the subkeys under:

HKEY_CURRENT_USERS\Software\VendorName - (i.e. Adobe, Microsoft etc.)

In step S45 the changes or "critical" changes are encrypted for security purposes. The encryption technique used can comprise any conventional encryption technique such as Blowfish. In step S46 the changes are covertly or secretly transmitted to the remote monitoring party. In step S47 it is then determined whether the transmission has been successful. If not, in step S54 retransmissions can be periodically retried. If there is still no successful transmission the security program can terminate in step S53.

If transmission is successful, in step S48 the data in the security program data key in the registry is updated. At the remote monitoring party, in step S55 the changes are checked to determine whether there has been a security breach. Where the changes appear significant, the remote monitoring party may take the steps of contacting the computer user to determine that there has been a security breach e.g. whether the computer has been stolen. The remote monitoring party may however have been informed that the user's circumstances have changed and that configuration changes are to be expected and therefore the remote monitoring party will not take any

action and will simply update the configuration information kept for the computer.

The following gives two code fragments which can perform the step of setting the program to run once at start-up.

Code Fragment in C

```
/* load the path into the string szAppPath */
szAppPath=App.Path & "\\" & App.NicsApp & ".EXE"
/* Create a key in the registry at the required
location and return its address in hKey */
RegCreateKey(HKEY_LOCAL_MACHINE,
"Software\\Microsoft\\Windows\\CurrentVersion\\Run",
&hKey);
/* Name hKey "NicsApp" and set its value to szAppPath
and length to the length of szAppPath + 1 */
RegSetValueEx(hKey, "NicsApp", 0&, REG_SZ, szAppPath,
strlen(szAppPath)+1));
/*close and continue */
RegCloseKey(hKey);
```

Code Fragment in Visual Basic

```
Dim hKey as Long
Dim strRunCmd as String
'set the path for NicsApp
strRunCmd=App.Path & "\" & App.NicsApp & ".EXE"
'Create a key in the registry at the required location
and return its address in hKey
```

```
RegCreateKey(HKEY_LOCAL_MACHINE,
"Software\Microsoft\Windows\CurrentVersion\Run",
&hKey);
'Name hKey "NicsApp" and set its value to strRunCmd and
length to the length of strRunCmd + 1
RegSetValueEx(hKey, "NicsApp", 0&, REG_SZ, ByVal
strRunCmd, Len(sRunCmd)+1));

'Close and continue
RegCloseKey
```

The steps performed by the security program in Figure 6 are implemented covertly to avoid warning any potential thief or unauthorised person that their activities have been logged. Thus, not only is the transmission of the changes undertaken covertly, but also the program operates covertly so as to be invisible to the user.

Figure 7 is a flow diagram illustrating step S46 of Figure 6 in more detail.

In step S60 it is determined during bootup whether there is a network connection or a modem present. In step S61 the type of connection is then determined if there is no connection, in step S62 the program terminates. If there is a network connection, in step S67 the changes are transmitted over the network. In step S66 the security program then deletes the connection log and removes all records of the connection and the program terminates in step S62.

If the modem is present, in step S63 it is determined whether there is an internet connection via an internet service provide (ISP). If so, in step S65 the changes are transmitted over the internet. If not, the changes are transmitted by directly dialling the remote monitoring equipment and making a direct connection in step S64. Whenever a modem is used, in order to ensure secrecy, the modem loud speaker is turned off using the command "ATD0". Then in step S66 the connection log is deleted and all records of the connection is removed. The program then terminates in step S62.

If the connection is made via the direct dial technique in step S64, not only can the remote monitoring party receive the changes in the configuration information but also they can obtain the telephone number from which the connection was made using the caller ID facility provided by telecommunications networks. Thus, this information can be used to identify the location of the computer should this be necessary in order to trace a security breach e.g. theft of the computer.

The embodiment of the present invention described in reference to Figures 3 to 7 can be used on computers which have any type of communications link e.g. modem, ISDN terminal, or network card. When the computer is connected to a network, the server in the network can intercept the transmitted changes in order to filter them and maintain an audit of the software and hardware of the

computers in the network. Such an embodiment will now be described with reference to Figures 8 to 10.

Figure 8 is a schematic diagram of a computer network in which clients 21, 22 and 23 are connected over a network 20 to a server 24 and a communications link 25. In each of the clients the security program 21b, 22b and 23b is stored in the respective registry 21a, 22a and 23a. In the server similarly, the security program 24b is stored in the server registry 24a. The server 24 additionally includes an administration program 24c for carrying out administration duties as will be described hereinafter in more detail. The communications link 25 provides a means of communication to a remote monitoring party 26 for monitoring changes in the configuration parameters of the computers 21, 22 and 23 of the network.

Figure 9 is a flow diagram illustrating the setting up of the system. In step S70 the security program is installed on the server. In step S71 the administration program is installed on the server. In step S72 the administration program causes the deployment of the security program to the clients. In step S73 the clients install and run the security program as has been described hereinabove with reference to the first embodiment. In step S74 the server receives the configuration information from the clients and collates this to form audit information. Thus the manager operating the server is able to automatically obtain an audit of the hardware and software provided in the network. Further, as will be described hereinafter the

audit information is automatically updated when changes in the configuration information is received from the clients. Thus the manager of the network has a completely updated audit automatically provided.

Figure 10 is a flow diagram illustrating the operation of the embodiment. In step S80 when configuration changes are made at a client, in step S81 the client transmits the changes. The server receives the changes and updates the audit information. This may not be necessary if the audit information has already been changed. For example, if the manager has already been asked permission for a computer to move location, e.g. change a network address, the manager may manually enter this in the audit information and thus when the changes are received, the audit information may not require updating.

In step S83, the server is able to filter the changes in order to filter out any changes which are not pertinent to security. Such a decision may be based upon network parameters. For instance, changes which only indicate local movement of the computers may be filtered out since this merely indicates local mobility of the computers within the office and therefore this information need not be passed on to the remote monitoring party. In step S84 the server will then transmit any changes after filtering to the remote monitoring party.

As can be seen in this embodiment, the supervision by the server and the monitoring by the remote monitoring

party effectively provides two levels of monitoring. This allows for decisions to be made regarding information on changes at two different levels i.e. at a local level and at a remote level.

Because the server is able to access the register of the clients, the administration program is also able to check to determine whether the audit information matches the information in the registry of the clients. If there is a discrepancy, it indicates that the security program has not successfully transmitted the changes to the server. The manager of the network will then be able to investigate the reasons for this.

Although the embodiments described hereinabove are require a means of communication with the remote monitoring equipment, the present invention is not limited as such. In another embodiment of the present invention, if the security program is unable to transmit the changes within a time period of for example 24 to 48 hours, it will generate a program packet which includes the changes and a self executable program module much like a virus. This will be copied onto the first n disks loaded into the disk drive of the computer, where n is some predetermined number. When the disk with the program packet is inserted into another computer, the packet will determine whether the computer has a communications link available. If it does, the computer packet will launch itself and transmit the changes to the remote monitoring party using this "host" computer. The

program packet will then remove all traces of itself. If the "host" computer does not have a communications link available, the program packet will replicate onto n floppy disks inserted into the computer in order to be passed onto other computers to repeat the exercise.

The number of "generations" of this "virus" can be limited in order to limit the spread.

Although the embodiments of the present invention have been described as being implemented when the computer is booted up, the present invention is not limited to this. A computer program can run periodically and/or when the computer is booted up.

Further, although the embodiments of the present invention have been described with reference to computers, the present invention is not limited to this. The present invention is applicable to any apparatus such as mobile telephones, intelligent peripheral devices such as printers, set top boxes, cars, boats or yachts, and aeroplanes.

In the embodiments it has been described that the computer program is hidden (in the registry). This provides an added level of security but the computer program could be stored more conventionally as a file in a folder.

The configuration information which is monitored in the present invention can comprise any configuration information which can identify a machine, such as hardware, software, and user parameters. The user parameters particularly provide information on a pattern

of use and thus provide very specific configuration information. When equipment is used without authority e.g. stolen, a user will typically enter many configuration parameters which will identify the user. These will be transmitted to the remote monitoring party enabling a rapid identification of the unauthorised user.

Although the present invention has been described hereinabove, with reference to specific embodiments, it will be apparent for the skilled person in the art that modifications may be made without departing from the spirit and scope of the present invention.

CLAIMS:

1. A security method for apparatus having storage means for storing configuration information for the apparatus, the method comprising:

keeping a record of configuration information for said apparatus at a monitoring station;

monitoring, by said apparatus, changes in said configuration information for said apparatus; and

transmitting the changes in said configuration information to said monitoring station.

2. A security method according to claim 1, including the step of determining if any said changes in said configuration information are pertinent to security, wherein the transmission step transmits only the pertinent changes.

3. A security method according to claim 1 or claim 2, including initial steps of registration by a user of said apparatus with said monitoring station by submitting manually entered configuration information for said apparatus, automatically transmitting said configuration information to said monitoring station, and comparing the manually submitted configuration information with the transmitted configuration information.

4. A security method according to any preceding claim, wherein said configuration information includes information on hardware components of said apparatus.

5. A security method according to any preceding claim, wherein said configuration information includes information on the use of said apparatus by a user.

6. A security method according to any preceding claim, wherein said apparatus includes processing means, and said configuration information includes information on programs implemented by said processing means.

7. A security method according to any preceding claim including the step of updating the stored configuration information following transmission of the changes.

8. A security method according to any preceding claim, including performing a security check for said apparatus and updating the kept record of configuration information for said apparatus if said security check reveals no security breach.

9. A security method according to any preceding claim, wherein the changes in said configuration information are transmitted covertly.

10. A security method according to any preceding claim, wherein said apparatus includes transmission means which transmits the changes in said configuration information to said monitoring station.

11. A security method according to any one of claims 1 to 9, wherein said apparatus covertly outputs said changes in said configuration information in association with information or instructions intended for input to another apparatus, if the other apparatus has means for transmission to said monitoring station the changes are thereby transmitted, and if not the changes are output in association with information or instructions intended for another apparatus, and the latter step is repeated.

12. A security method according to claim 11, wherein said apparatus and said another apparatus covertly output said changes on a storage medium in association with a file.

13. A security method according to claim 12, wherein said apparatus and said another apparatus comprise computers and said changes are attached to said file as executable code for causing said transmission.

14. A security method according to any preceding claim wherein said monitoring and transmission steps take place periodically and/or when said apparatus is initialised.

15. A security method according to any preceding claim, wherein said apparatus includes processing means for implementing programs and said monitoring step is implemented by said apparatus when said processing means

implements a program module covertly stored in said apparatus.

16. A security method according to any preceding claim, including the step of encrypting the changes before transmission and decrypting the received encrypted changes at said monitoring station.

17. Apparatus for use in the method of any one of claims 1 to 9 comprising:

processing means for determining configuration information for said apparatus;

storage means for storing said configuration information;

wherein said processing means is adapted to compare current configuration information with the stored configuration information and to determine any changes;

the apparatus including means responsive to said processing means for outputting said changes for transmission to a monitoring station.

18. Apparatus according to claim 17, wherein said processing means is adapted to determine any changes, if any, which are pertinent to security and said output means is adapted to output only the pertinent changes.

19. Apparatus according to claim 17 or claim 18, wherein said processing means is adapted to control said output

means to initially output said configuration information for transmission to said monitoring station.

20. Apparatus according to any one of claims 17 to 19, wherein said storage means is adapted to store configuration information including information on hardware components of said apparatus.

21. Apparatus according to any one of claims 17 to 20, wherein said storage means is adapted to store configuration information including information on the use of said apparatus by a user.

22. Apparatus according to any one of claims, 17 to 21, wherein said storage means is adapted to store configuration information which includes information on programs implemented by said processing means.

23. Apparatus according to any one of claims 17 to 22, wherein said processing means is adapted to update the stored configuration information following output of the changes.

24. Apparatus according to any one of claims 17 to 23, wherein said outputting means is adapted to transmit said changes to said monitoring station.

25. Apparatus according to any one of claims 17 to 23, wherein said outputting means is adapted to output said

changes together with instructions for their transmission to said monitoring station as a packet in association with information or instructions intended for input to another apparatus, whereby if said another apparatus has means for transmission to said monitoring station the changes are thereby transmitted, if not the packet is output in association with information or instructions intended for another apparatus, and so on until transmission occurs.

26. Apparatus according to claim 25, wherein said outputting means is adapted to output said packet covertly in association with a file.

27. Apparatus according to claim 26, comprising a computer, wherein said outputting means is adapted to attach said packet as executable code to said file.

28. Apparatus according to any one of claims 17 to 27, wherein said outputting means is adapted to output said changes so as to ensure that said changes are covertly transmitted to said monitoring station.

29. Apparatus according to any one of claims 17 to 28, wherein said processing means is adapted to determine the changes and to control said outputting means to output periodically and/or when said apparatus is initialised.

30. Apparatus according to any one of claims 17 to 29, wherein said storage means is adapted to covertly store a program module for the control of said processing means, and said processing means is adapted to implement said program module to determine the changes and to control said outputting means.

31. Apparatus according to any one of claims 17 to 30, including means for encrypting the changes before being output by said output means.

32. A storage medium storing instructions for controlling a processing apparatus to be configured in accordance with any one of claims 17 to 31.

33. Processor implementable instructions for controlling a processing apparatus to be configured in accordance with any one of claims 17 to 31.

34. A monitoring station for use in the method of any one of claims 1 to 16, including storage means for storing a record of configuration information for one or more remote apparatus, means for receiving said changes in said configuration information, and means for processing said changes.

35. A monitoring station according to claim 34, including means for decrypting said changes received in encrypted form.

36. A monitoring station according to claim 34 or claim 35, including means for initially receiving and storing said configuration information.

37. A monitoring station according to claim 36, including means for inputting configuration information submitted by a user of a said apparatus, and means for comparing the submitted configuration information with the stored configuration information to detect any discrepancies.

38. A storage medium storing instructions for controlling a processing apparatus to be configured in accordance with any one of claims 34 to 37.

39. Processor implementable instructions for controlling a processing apparatus to be configured in accordance with any one of claims 34 to 37.

40. An automatic audit method comprising:

transmitting apparatus configuration information from apparatus to an auditor station;

monitoring, by the apparatus, changes in said configuration information for said apparatus; and

transmitting said changes to said auditor station.

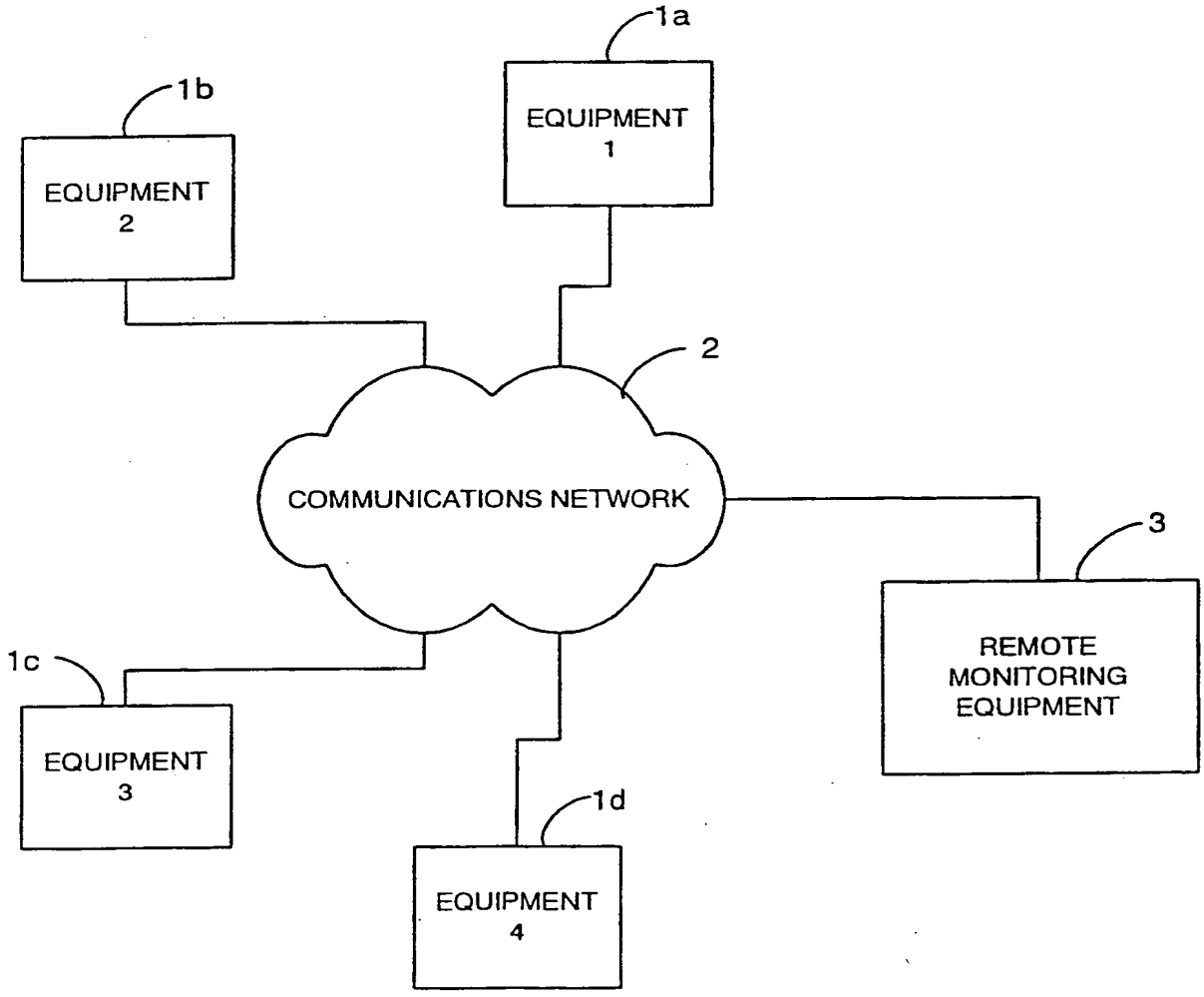

1a
EQUIPMENT 1
1b
EQUIPMENT 2
2
COMMUNICATIONS NETWORK
3
REMOTE MONITORING EQUIPMENT
1c
EQUIPMENT 3
1d
EQUIPMENT 4

Fig 1

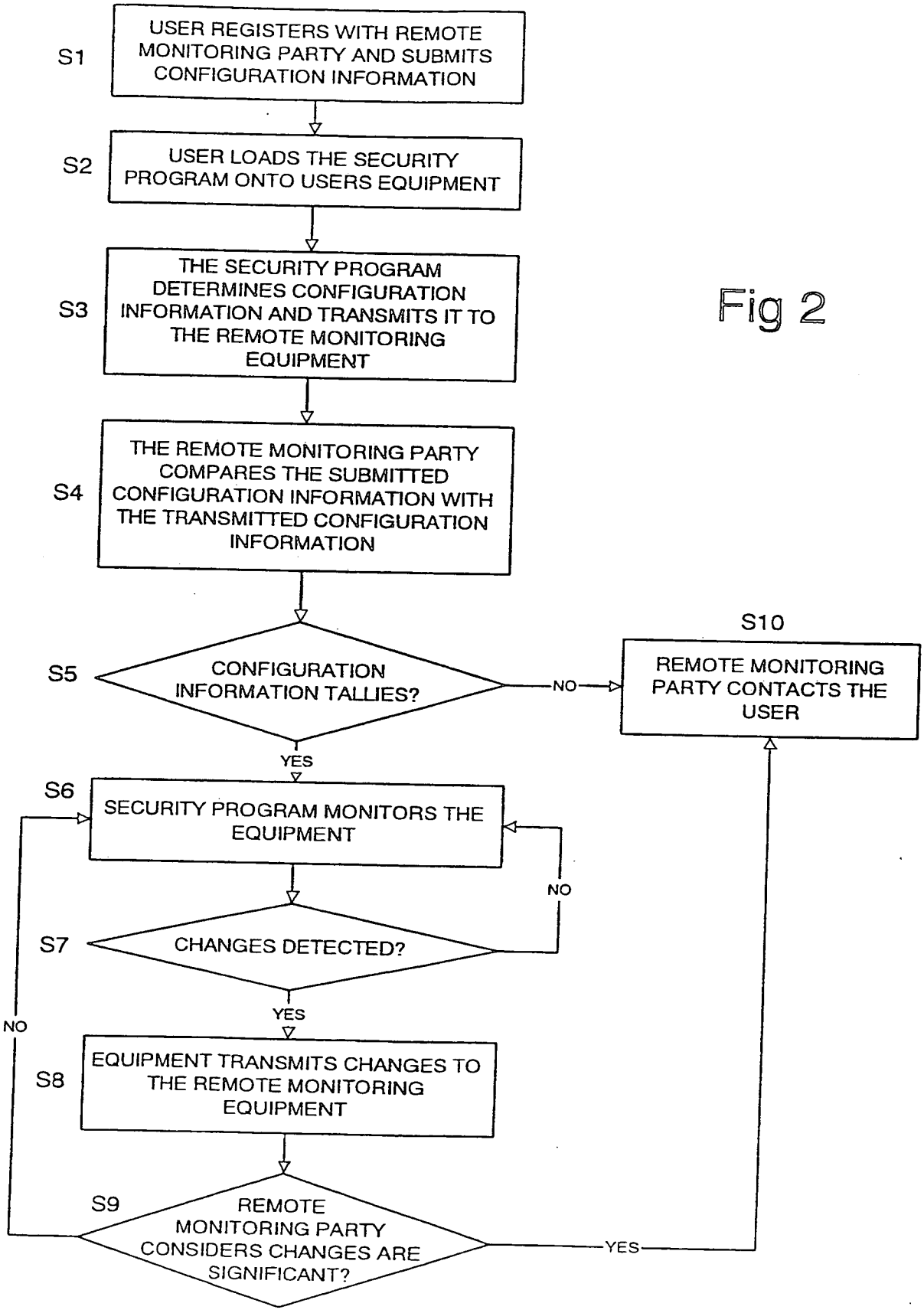

S1
USER REGISTERS WITH REMOTE MONITORING PARTY AND SUBMITS CONFIGURATION INFORMATION
S2
USER LOADS THE SECURITY PROGRAM ONTO USERS EQUIPMENT
S3
THE SECURITY PROGRAM DETERMINES CONFIGURATION INFORMATION AND TRANSMITS IT TO THE REMOTE MONITORING EQUIPMENT
S4
THE REMOTE MONITORING PARTY COMPARES THE SUBMITTED CONFIGURATION INFORMATION WITH THE TRANSMITTED CONFIGURATION INFORMATION
S5
CONFIGURATION INFORMATION TALLIES?
NO
S10
REMOTE MONITORING PARTY CONTACTS THE USER
YES
S6
SECURITY PROGRAM MONITORS THE EQUIPMENT
NO
S7
CHANGES DETECTED?
YES
NO
S8
EQUIPMENT TRANSMITS CHANGES TO THE REMOTE MONITORING EQUIPMENT
S9
REMOTE MONITORING PARTY CONSIDERS CHANGES ARE SIGNIFICANT?
YES

Fig 2

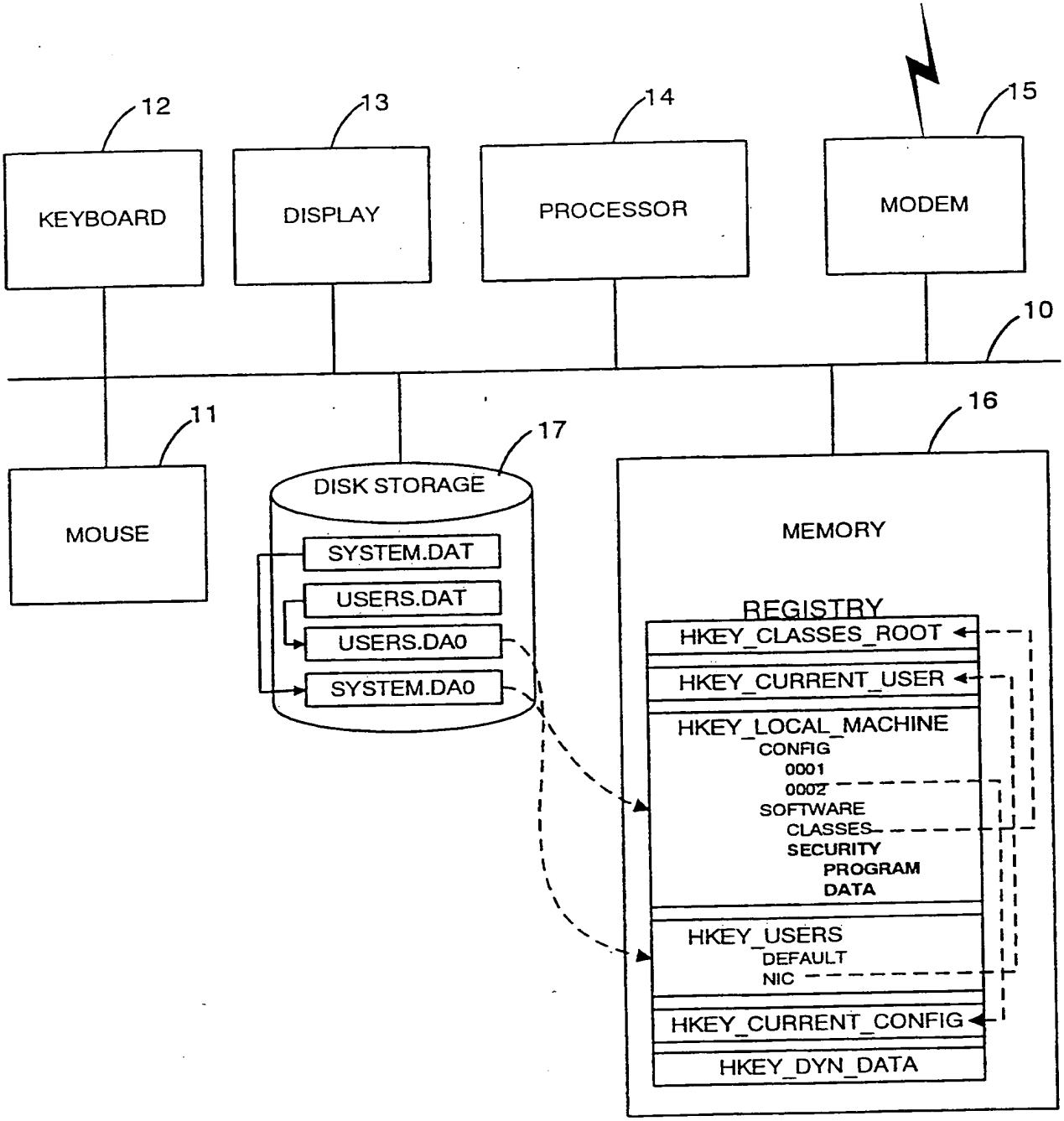

12
13
14
15
KEYBOARD
DISPLAY
PROCESSOR
MODEM
10
11
16
17
MOUSE
DISK STORAGE
SYSTEM.DAT
USERS.DAT
USERS.DA0
SYSTEM.DA0
MEMORY
REGISTRY
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
CONFIG
0001
0002
SOFTWARE
CLASSES
SECURITY
PROGRAM
DATA
HKEY_USERS
DEFAULT
NIC
HKEY_CURRENT_CONFIG
HKEY_DYN_DATA

Fig 3

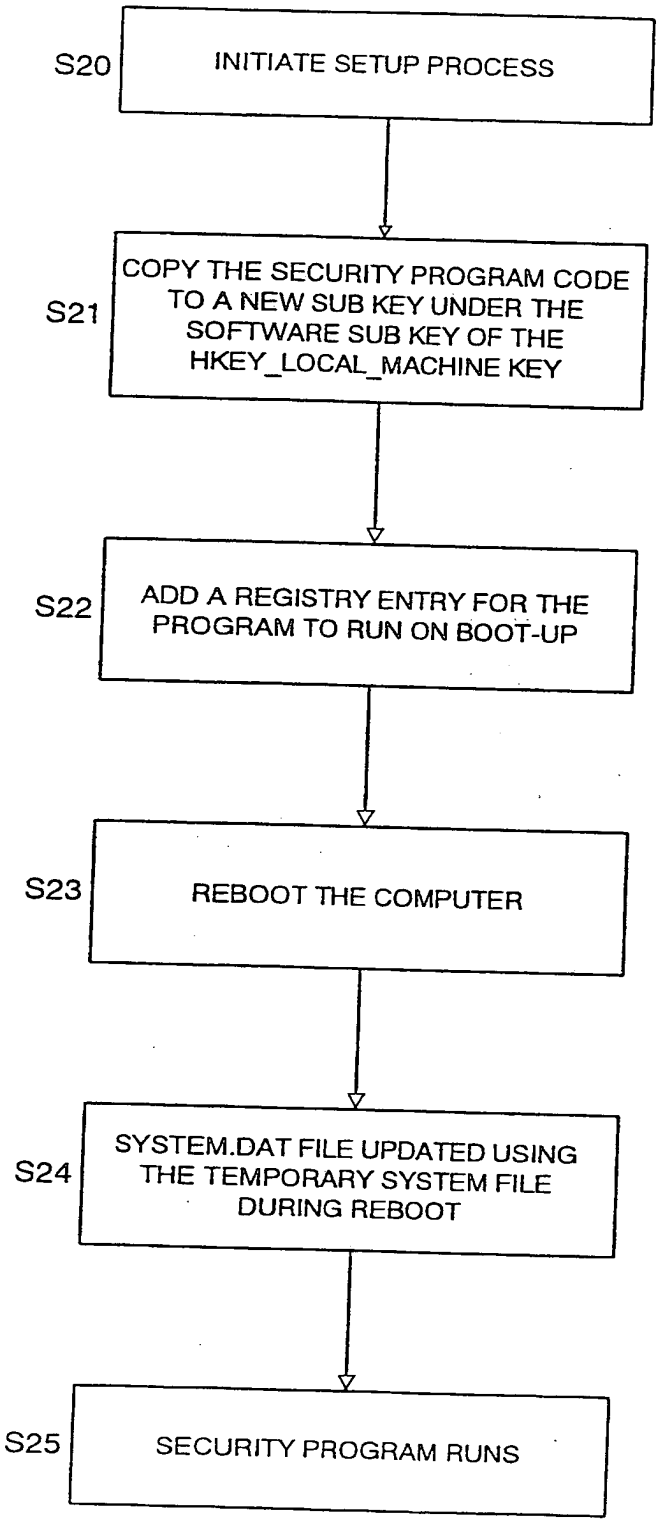

S20
INITIATE SETUP PROCESS
S21
COPY THE SECURITY PROGRAM CODE TO A NEW SUB KEY UNDER THE SOFTWARE SUB KEY OF THE HKEY_LOCAL_MACHINE KEY
S22
ADD A REGISTRY ENTRY FOR THE PROGRAM TO RUN ON BOOT-UP
S23
REBOOT THE COMPUTER
S24
SYSTEM.DAT FILE UPDATED USING THE TEMPORARY SYSTEM FILE DURING REBOOT
S25
SECURITY PROGRAM RUNS

Fig 4

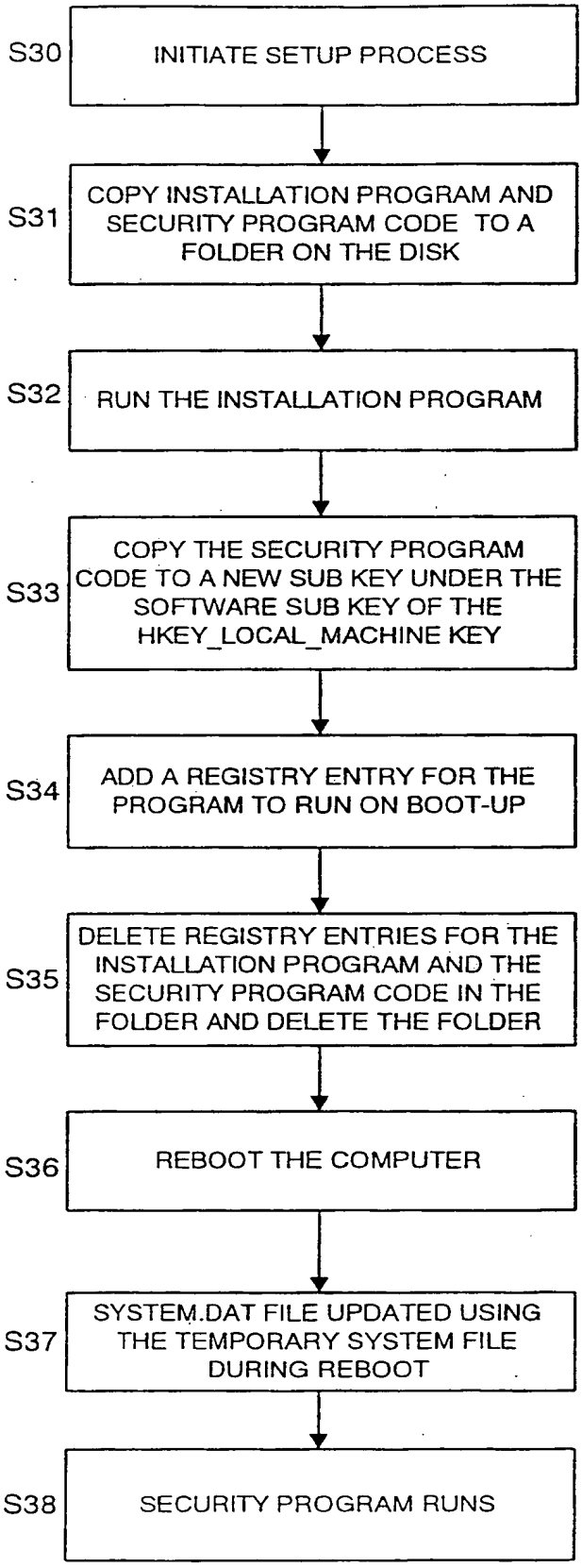

S30
INITIATE SETUP PROCESS
S31
COPY INSTALLATION PROGRAM AND SECURITY PROGRAM CODE TO A FOLDER ON THE DISK
S32
RUN THE INSTALLATION PROGRAM
S33
COPY THE SECURITY PROGRAM CODE TO A NEW SUB KEY UNDER THE SOFTWARE SUB KEY OF THE HKEY_LOCAL_MACHINE KEY
S34
ADD A REGISTRY ENTRY FOR THE PROGRAM TO RUN ON BOOT-UP
S35
DELETE REGISTRY ENTRIES FOR THE INSTALLATION PROGRAM AND THE SECURITY PROGRAM CODE IN THE FOLDER AND DELETE THE FOLDER
S36
REBOOT THE COMPUTER
S37
SYSTEM.DAT FILE UPDATED USING THE TEMPORARY SYSTEM FILE DURING REBOOT
S38
SECURITY PROGRAM RUNS

Fig 5

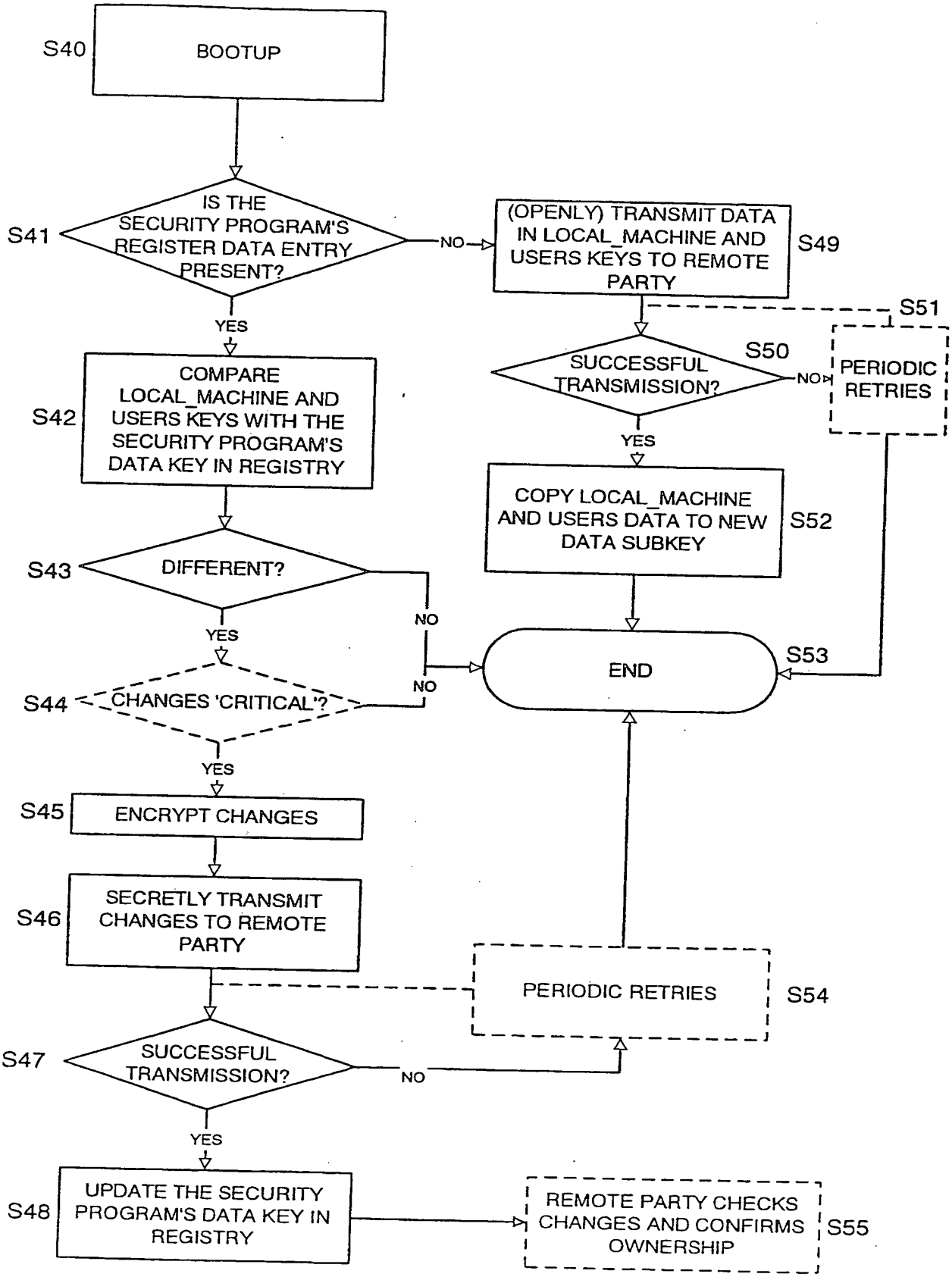

S40
BOOTUP
S41
IS THE SECURITY PROGRAM'S REGISTER DATA ENTRY PRESENT?
NO
(OPENLY) TRANSMIT DATA IN LOCAL_MACHINE AND USERS KEYS TO REMOTE PARTY
S49
S51
PERIODIC RETRIES
S50
SUCCESSFUL TRANSMISSION?
NO
YES
YES
S42
COMPARE LOCAL_MACHINE AND USERS KEYS WITH THE SECURITY PROGRAM'S DATA KEY IN REGISTRY
COPY LOCAL_MACHINE AND USERS DATA TO NEW DATA SUBKEY
S52
S43
DIFFERENT?
NO
YES
S44
CHANGES 'CRITICAL'?
NO
END
S53
YES
S45
ENCRYPT CHANGES
S46
SECRETLY TRANSMIT CHANGES TO REMOTE PARTY
PERIODIC RETRIES
S54
S47
SUCCESSFUL TRANSMISSION?
NO
YES
S48
UPDATE THE SECURITY PROGRAM'S DATA KEY IN REGISTRY
REMOTE PARTY CHECKS CHANGES AND CONFIRMS OWNERSHIP
S55

Fig 6

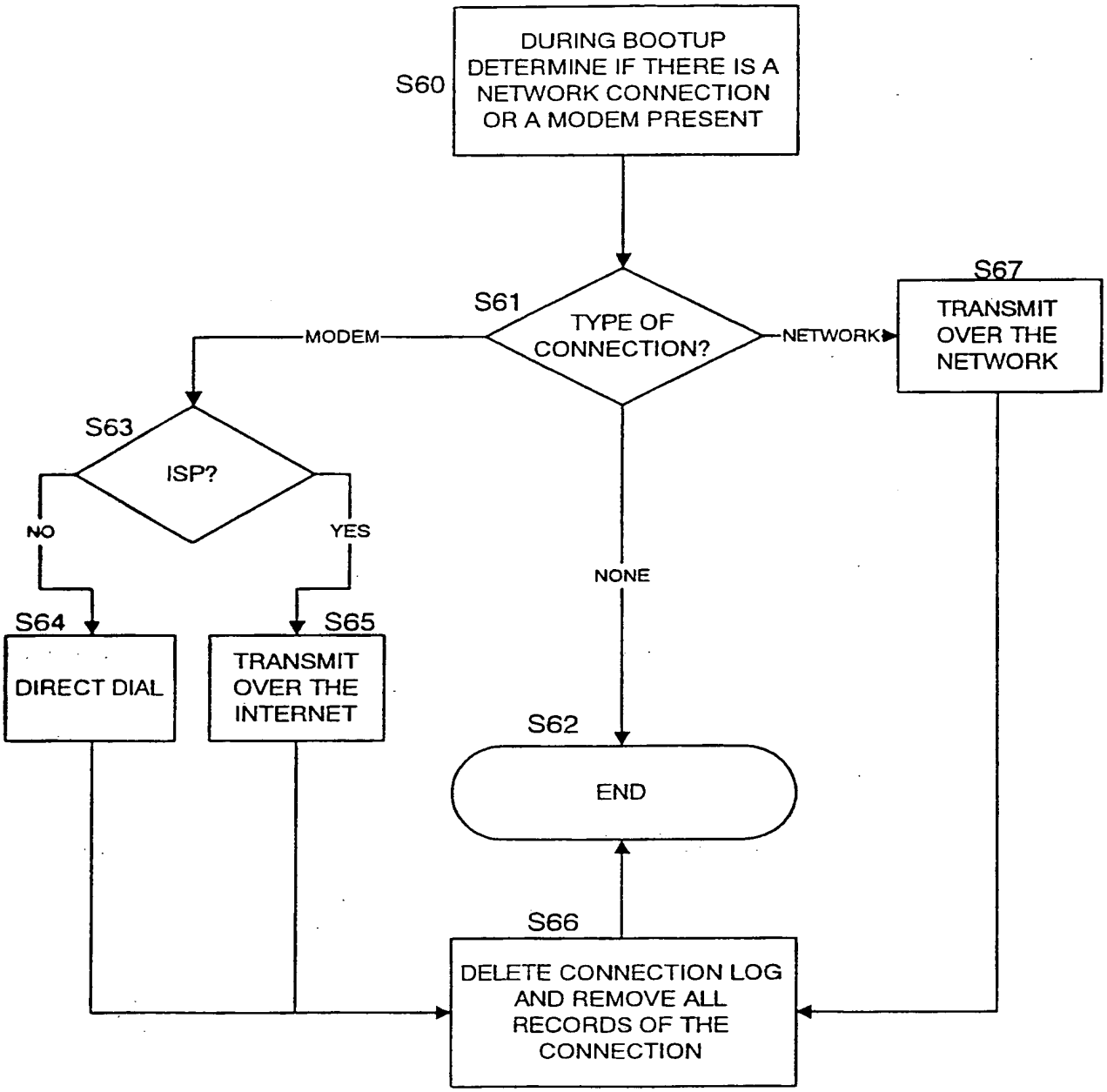

S60
DURING BOOTUP DETERMINE IF THERE IS A NETWORK CONNECTION OR A MODEM PRESENT
S61
TYPE OF CONNECTION?
MODEM
NETWORK
NONE
S67
TRANSMIT OVER THE NETWORK
S63
ISP?
NO
YES
S64
DIRECT DIAL
S65
TRANSMIT OVER THE INTERNET
S62
END
S66
DELETE CONNECTION LOG AND REMOVE ALL RECORDS OF THE CONNECTION

Fig 7

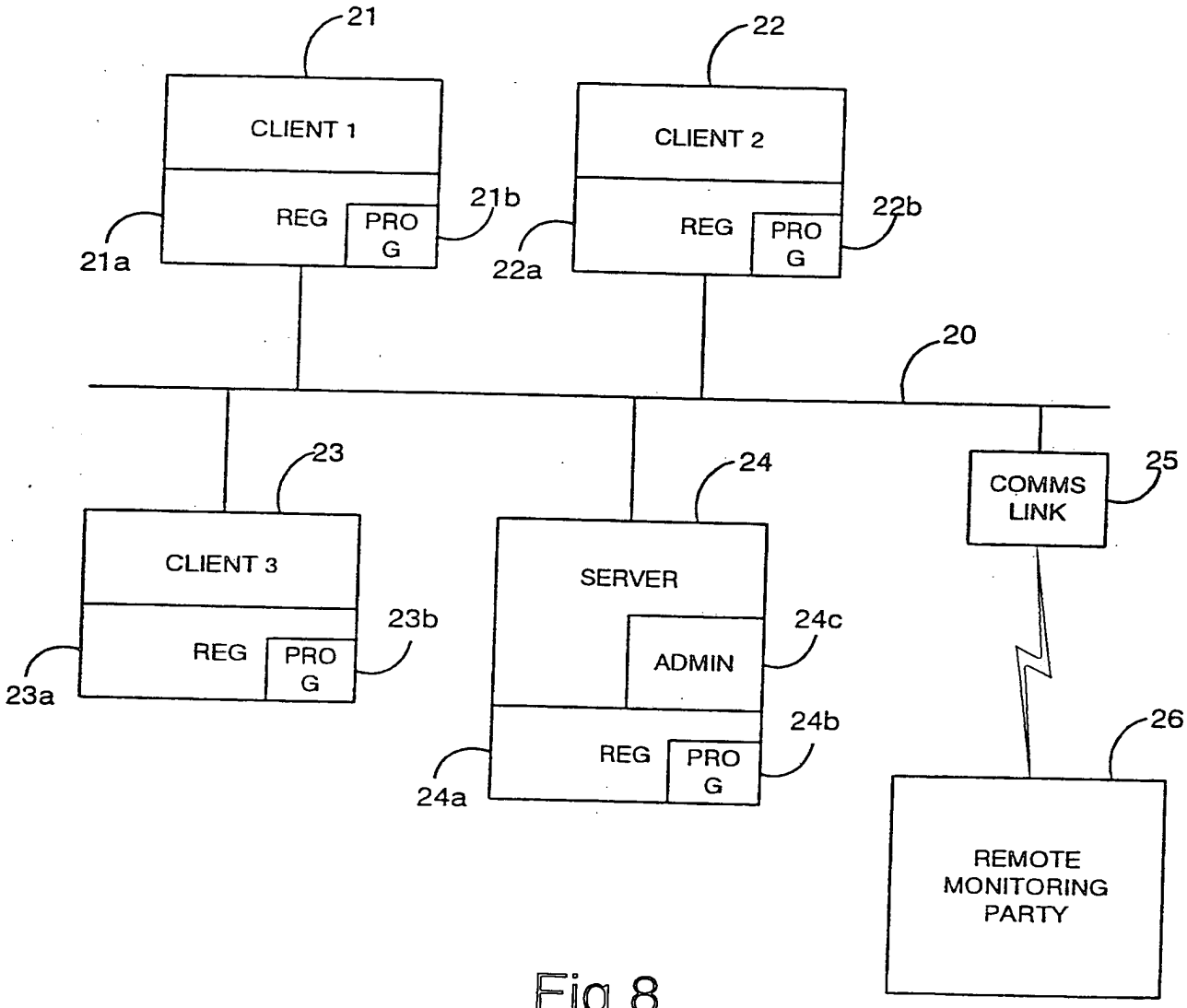

21
CLIENT 1
REG
PRO G
21b
21a
22
CLIENT 2
REG
PRO G
22b
22a
20
23
CLIENT 3
REG
PRO G
23b
23a
24
SERVER
ADMIN
24c
REG
PRO G
24b
24a
25
COMMS LINK
26
REMOTE MONITORING PARTY

Fig 8

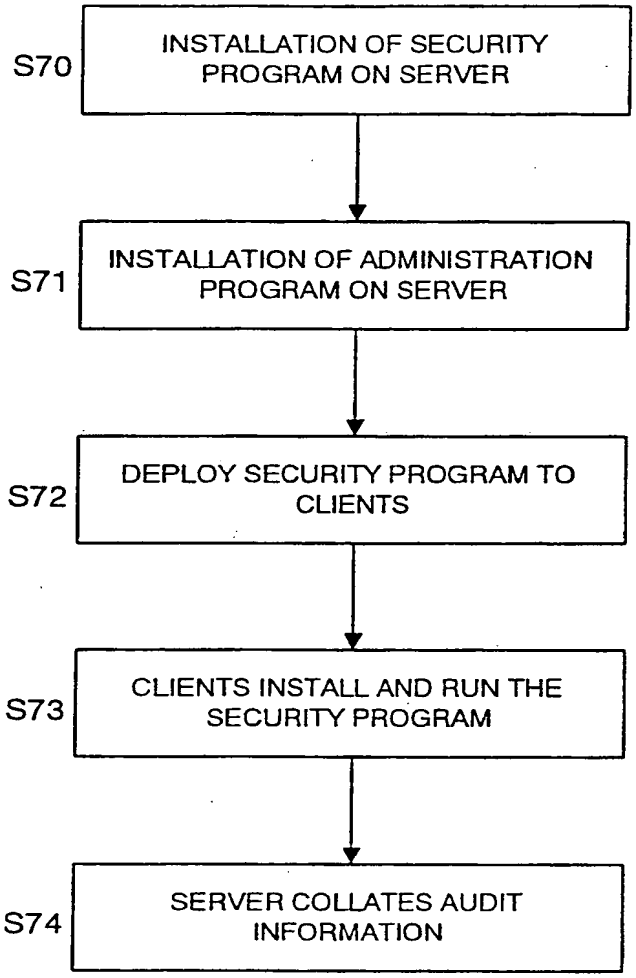

S70
INSTALLATION OF SECURITY PROGRAM ON SERVER
S71
INSTALLATION OF ADMINISTRATION PROGRAM ON SERVER
S72
DEPLOY SECURITY PROGRAM TO CLIENTS
S73
CLIENTS INSTALL AND RUN THE SECURITY PROGRAM
S74
SERVER COLLATES AUDIT INFORMATION

Fig 9

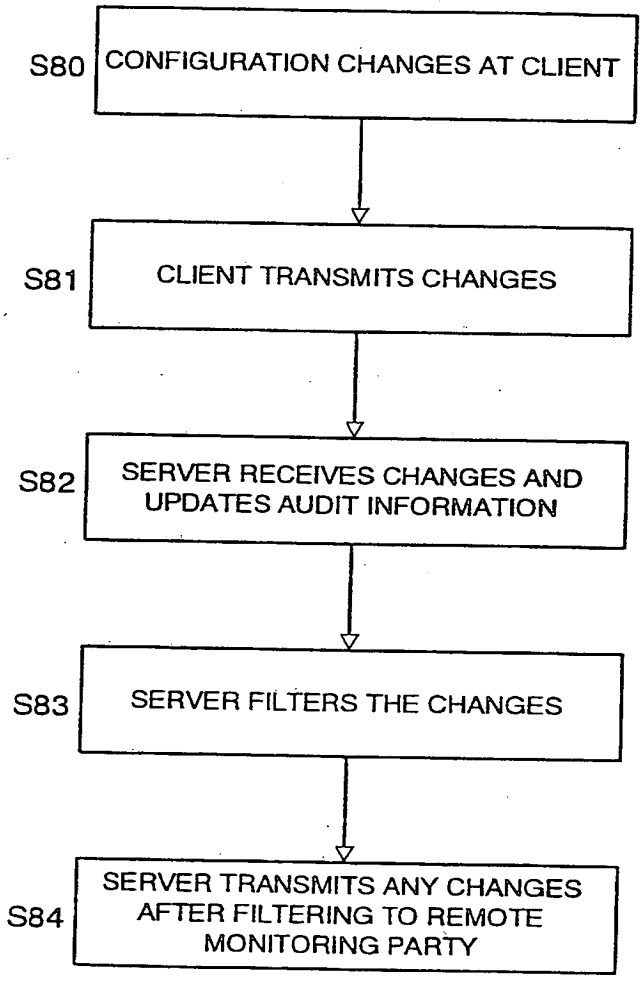

S80
CONFIGURATION CHANGES AT CLIENT
S81
CLIENT TRANSMITS CHANGES
S82
SERVER RECEIVES CHANGES AND UPDATES AUDIT INFORMATION
S83
SERVER FILTERS THE CHANGES
S84
SERVER TRANSMITS ANY CHANGES AFTER FILTERING TO REMOTE MONITORING PARTY

Fig 10

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 00/02082

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F11/22 G06F11/273 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 287 505 A (CALVERT NATHANIEL ET AL) 15 February 1994 (1994-02-15) abstract; claims 1-6	1-40

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 October 2000	10/10/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sarasua, L.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ational Application No
PCT/GB 00/02082

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5287505 A	15-02-1994	DE 68920462 D	23-02-1995
		DE 68920462 T	13-07-1995
		EP 0333620 A	20-09-1989
		JP 1243135 A	27-09-1989
		JP 1916596 C	23-03-1995
		JP 6044242 B	08-06-1994